

АЛЕКСАНДР МИРИДОНОВ

УВЕЛИЧЕНИЕ УТЕЧЕК БАЗ ДАННЫХ И АТАК ПРОГРАММ-ВЫМОГАТЕЛЕЙ СТАНОВИТСЯ ВСЕ БОЛЕЕ СЕРЬЕЗНОЙ ПРОБЛЕМОЙ ДЛЯ БИЗНЕСА

5 → **В КОНТЕКСТЕ AI** К новым вызовам кибермошенничества опрошенные Guide эксперты относят активное использование AI. «Уже есть новая матрица атак с использованием AI (MITRE Atlas), которую необходимо изучить экспертам в области ИБ для построения проактивных механизмов противодействия угрозам. Решения, основанные на AI для средств защиты, будут использоваться и командами защитников. Возникает новый виток щита и меча»,— акцентирует Дмитрий Узлов, руководитель отдела ИБ «Мобиус Технологии».

Развитие AI-технологий существенно снижает порог входа в «хакерскую сферу»: ее стало гораздо проще организовать, да и обходится она дешевле, говорит бэкенд-разработчик Филипп Щербанич. «Причем речь не только о серьезных взломщиках систем, но и о так называемых скрипт-кидди — людях, которые о взломе знают очень мало, но умеют пользоваться специальными готовыми программами. А AI-решения становятся для них одновременно и учебником, и инструктором по взлому»,— говорит IT-эксперт. Вместе с тем растет и количество инструментов для противостояния атакам. И это тоже происходит благодаря AI: например, уже есть системы, которые анализируют поведение сотрудников, и благодаря им можно предупредить попытку дипфейк-атаки.

Основные AI-угрозы в 2025 году будут по-прежнему связаны с фишингом. «В этом плане AI-инструменты очень полезны хакерам: многие работают удаленно, и их можно относительно легко обмануть, притворившись другим человеком (с помощью подделки аудио или видео). Собеседник уверен, что говорит с родственником, знакомым или начальником, но на „другом конце провода“ — мошенник. Для этого используются технологии дипфейка — с их помощью добываются важные доступы, пароли, секретная информация. Кроме этого, большие языковые модели применяют для имитации сообщений какого-нибудь человека: это тоже может быть очень актуально при фишинговых атаках. Тут злоумышленникам открываются серьезные возможности автоматизации данного процесса»,— рассказывает господин Щербанич.

Руководитель группы защиты инфраструктурных IT-решений «Газинформсервис» Сергей Полунин заострил внимание на доверие к информации: «С помощью ИИ можно изготовить фейковые документ, видео и аудио практический любой сложности. Проблема эта появилась довольно давно, но именно в связи с успехами того же ChatGPT, Gemini, Grok и подобных, она рискует вырасти до очень серьезных размеров».

КОНТУРЫ ЗАЩИТЫ До 2022 года основным источником утечек данных считались действия сотрудников, но затем ситуация изменилась — на первый план вышли внешние угрозы. «Однако в 2024 году вновь произошел рост инцидентов, связанных с внутренними нарушителями, включая умышленные утечки. Поэтому отдавать приоритет защиты внутреннего или внешнего контуров недостаточно, важно разрабатывать комплексную стратегию»,— отмечает генеральный директор «Эвритег» Сергей Тимошенко.

Кроме того, границы между внутренним и внешним контурами защиты размываются из-за облачных сервисов и удаленной работы. «Защита требуется на всех уровнях: от личных устройств до серверов. Приоритетом становится контроль внутреннего контура, так как ему традиционно доверяют больше, а угрозы изнутри (например, вредоносное ПО на устройствах сотрудников) могут быть более опасными. Основным трендом становится внедрение систем классов Endpoint Protection, DLP, возможно с элементами ИИ»,— отмечает Андрей Малов, директор по продукту «ТТК.Облако».

В целом перспективным подходом в контексте защиты по внутреннему контуру становится модель Zero Trust, предполагающая, что любая попытка доступа к данным проверяется вне зависимости от доверенного статуса пользователя, то есть даже если запрос исходит от администратора.

КОГДА УГРОЗА — СОТРУДНИК Человеческий фактор остается самой большой проблемой. «Почти 90% кибератак происходят из-за невнимательности или незнания сотрудников. Без регулярного обучения люди продолжают кликать по фишинговым ссылкам, использовать слабые пароли и передавать данные третьим лицам. Поэтому обучение должно быть не формальностью, а обязательным элементом безопасности»,— предупреждает генеральный директор компании «Фрикейк» Виталий Панов.

«По незнанию люди могут спросить у того же ChatGPT, насколько хороша та или иная идея, запросить оценку ее потенциала, генерацию новых идей на основе уже разработанных. Так может произойти утечка и раскрытие данных. Также известны случаи, когда работники компаний „скармливали“ для быстрой аналитики ИИ ряд секретных документов. В сеть спокойно просачивались те данные, которые должны были оставаться конфиденциальыми. Поэтому вопрос именно цифровой грамотности и безопасности сегодня ключевой»,— подчеркивает основатель холдинга The Business Pill Игорь Малинин.

Причем, даже если человек понял и принял все рекомендации, в стрессовой ситуации он будет действовать на эмоциях. «Именно на этом строится большинство атак. Фишинговые письма всегда провоцируют эмоциональный отклик, подавляя логическое мышление. Сочетание грамотного объяснения, мотивации и постоянной практики позволяет превратить сотрудников из главной уязвимости в надежный элемент системы защиты»,— подытожил специалист ГК Softline Николай Постнов. ■